ATTACHMENTS

Attachment 1	Attachment E of FBI affidavit for a warrant Returned emails lacking headers and footers,
Attachment 2	William Leonard's communications with ISOO re classification errors exposed in Drake pre-trial hearings
Attachment 3	Affidavits of Binney, Wiebe and Drake
Attachment 4	Information on "For Official Use Only" designation
	Wall Street Journal article Dec. 15, 2009
	President's memorandum to department and agency heads
	E.O. 13556

Roark v. U.S., Plaintiff Reply, Cross-Motion

Attachment E

Items to be Seized

Any items which constitute evidence, instrumentalities, or fruits of violation of Title 18, United States Code, Sections 371 (Conspiracy To Commit An Offense Against The United States), 793 (Unlawful Disclosure of Classified National Defense Information), and 798 (Unlawful Disclosure of Classified Information), including specifically:

1. U.S. government documents, classified documents (including classified documents missing headers and footers), national defense intelligence documents and papers, and other documents relating to the National Security Agency (NSA).

2. Papers or documents relating to the transmittal of U.S. government documents, national defense and classified intelligence to representatives of the news media, or individuals not authorized to receive the information;

3. Computer hardware, meaning any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as floppy disks, compact disks/CD-roms, hard disk drives, flash drives, tapes, or similar data storage devices/media); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections); and any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as "dongles," keycards, physical keys, and locks).

4. Computer software, meaning any and all information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

5. Computer-related documentation, meaning, any written, recorded, printed, or electronically-stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

6. Computer passwords and data security devices, meaning any devices, programs, or data – whether themselves in the nature of hardware or software – that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any

on FF's T-cubed "spins" as they wind out in 90 day increments. 4/06 Re E

They are using (in part) J2EE as glueware/middleware in an attempt to stitch together something that can be ostensibly used in a "multi-tier" environment. Engebretson job

But... techy

Attempting to break that "nut" without clearances or thru teaming arrangements is daunting at best as there are a LOT of players in this marketplace doing "integration", web services, and application hosting and messaging.

And...

J2EE is no silver bullet, believe me.

There are still issues with maintainability, scalability, and performance (especially at the enterprise level) and especially if the developers attempt to "tweak" or reinvent what already exists within the J2EE environment.

I would go with the parts of gov't that actually use their websites for services that are practical and of benefit to our citizens. :-)

Short of teaming/hooking up with a web services provider in the IC (and with the other option of web monitoring services in a Quality of Service role), have him check out the government's "e-Gov" initiatives, too.

Must angle what "differentiates" them too, in a crowded marketplace.

Roark v. U.S., Attachment 1

Diane: FF's Xformation 3.0 (aka TU*) is heavy into J2EE. The major companies supporting it r Essex, Booz, and to a lesser extent, Boing (the omitted e is intentional). However, the funding of the programs is done via task orders and the task orders r typically solid for just 90 days. If there's no useful light at the end of the 90-day tunnel, future $ r at risk. I'm aware of funded programs being "de-obligated" in order to churn $ for TU*. If he's interested in living on the edge (as it looks like will be the case during Alexander's tenure), he may want to press some flesh with those companies.

Anybody see or read about the Bush press conference today? 1/27/06

>>> Yes.

He is now saying that the 1978 Foreign Intelligence Surveillance Act is outdated, given the realities of 2006!

>>> Agree, it is outdated! And I tried convincing KP of that fact 7 years ago. FISA is fine for an analog, point-to-point comms world as written. However, it needs to be brot into the 21st century where for the digital, packet-switched world of today. And once it's recaste, then U18 needs to be drastically revised! That thing still refers to office authorities for offices that no longer exist (e.g. DDO) and has no mention of the role played by the NID! Shear lunacy now that u asked.

Huh?

Does that REALLY mean the Executive Branch can ignore what it deems unilaterally is now outdated, even if it is the law, simply because the Executive Branch says so?

>>> No, BUT he is right!

And what about the fact that FISA has been amended SINCE 1978, and most recently as a result of the Patriot Act?!

Like the provision in the Patriot Act that further expands FISA to permit "roving wiretap" authority, thus allowing for the interception of ANY communications made to or by an intelligence target without specifying the particular telephone line, the computer or even the facility to be monitored!

And...

As well...

The Patriot Act removed the pre-existing statutory requirement that the government prove the surveillance target is "an agent of a foreign power" before obtaining a pen register/trap and trace surveillance order under FISA and can now obtain a pen register/trap and trace device "for any investigation to gather foreign intelligence information," without showing that the device has, is or will be used by a foreign agent or by an individual engaged in international terrorism or clandestine intelligence activities!

So...

Seems rather unambiguous to me that Congress and the Courts have clearly NOT unduly restrained (or constrained) the Executive Branch hardly at all now, in pursuit of its legitimate national security authorities and responsibilities, for monitoring the activities of foreign powers and their agents, and now goes even further with the removal of the "foreign power" requirement

Roark v. U.S., Attachment 1

for pen register/trap and trace surveillance!!

What is the problem, then?

>>> It's not written for a digitally-connected world. It's written for an old comms paradigm.

I just don't get it!

However, the Patriot Act DOES include a provision prohibiting the use of a FISA pen register and trace surveillance under ANY circumstances against a United States citizen where the investigation is conducted "solely on the basis of activities protected by the First Amendment."

Is that what is outdated?!

>>> It might be, depending on the legal definition of a "pen register." Since u won't find that in the Constitution, it's up to interpretation.

Seems pretty up to date to me!

Why then the need to bypass FISA???!!!

And...

Any of you hear about the following?

That Representative Rush D. Holt, Democrat from New Jersey, and a member of HPSCI apparently complained over what Holt described as deception by Gen Alexander??!

Apparently, Holt visited FF in early December 2005 for a briefing given by Alexander and FF lawyers about the protection of privacy for Americans.

He was apparently assured that FF singled out Americans for eavesdropping ONLY under warrants from the Foreign Intelligence Surveillance Court!!

Is it possible that FF lied to Holt, or the lawyers at FF were simply quoting the law??!!

>>> Sure it's possible. FF lied to Congress and its staff numerous times when we were working in the SARC. Why wud the wolf change colors when he knew there already had been a tempest brewing with Tice?

So...

Who is advising who, here??!

FISA PERMITS WARRANTLESS WIRETAPPING UNDER CERTAIN CONDITIONS!!!

Besides the 72 hour condition and the 15 day condition when Congress has declared war is the following:

The President may authorize, through the Attorney General, electronic surveillance **WITHOUT** a court order for a **period of one year** provided it is only for foreign intelligence information targeting foreign powers as defined by 50 U.S.C. §1801(a)(1),(2),(3) or their agents; and there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party.

The Attorney General IS required to make a certification of these conditions under seal to the FISA Court and report on their compliance to the HPSCI and SSCI.

What is the problem?!

The compliance issue?!

>>> The problem is an outdated law, and KP was the problem person who wudn't press to have it modernized legally when I pressed him on it for several years. His lame excuse was that every time an attempt was made to loosen it, the attempt backfired and it got tighter. el

And yes...

Under FISA, anyone who engages in electronic surveillance except as authorized by statute is subject to both criminal penalties and civil liabilities.

He's trying to say (and he's been well coached by Mikey/Pasha on this) that the process is outdated and sufficiently unresponsive to today's time-sensitive requirements. Well, yeah, if you accept the fact that the implementation is sophomoric and in need of overhaul. HOWSOMESOEVER (as some rednecks say), that is a lame excuse and he will be rudely awakened when hearings begin (I hope). If he's basing his defense on a an outdated business process and hasn't make any effort to improve it, it's a specious argument at best and won't hold up under any reasonable scrutiny.

What ethics?!

I checked with my sources on this one with respect to the books and got the sardonic "Right" response when I asked.

Said everything to me.

It is a mess.

So Alex is VERY constrained right now in terms of the monies he can move to TU.

And yes...

He thought he could finesse getting around the hoops given his "new" approach to acquisition with SPINs.

Also...

Corporate "taxing" has been a method in the past to pay for higher priority things.

And what about the CBJB?

Largely ignored.

Roark v. U.S., Attachment 1

INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES and RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW, ROOM 100 WASHINGTON, DC 20408-0001
www.archives.gov/isoo

NATIONAL ARCHIVES

December 26, 2012

J. William Leonard
P.O. Box 2355
Leonardtown, MD 20650

VIA E-MAIL

Dear Mr. Leonard,

I am responding to your letter of July 30, 2011, in which you asked that I, in accordance with my assigned duties under Executive Order 13526, "Classified National Security Information" ("the Order"), consider and take action with regard to what you viewed as a violation of the Order. Specifically, you requested I "ascertain if employees of the United States Government, to include the National Security Agency (NSA) and the Department of Justice (DOJ), have willfully classified or continued the classification of information in violation of the Order" in the matter of *United States v. Thomas A. Drake*. I have concluded my inquiries into this matter, having consulted with the above-mentioned agencies, drawn upon the Order, its implementing Directive, and examined relevant portions of each agency's security regulations, and now share with you my findings and observations.

With regard to your complaint, I conclude that neither employees of the Department of Justice nor of the National Security Agency willfully classified or continued the classification of the "What a Wonderful Success" document in violation of the Order. I wish to note that your complaint suggests this was done "in the matter of *United States v. Thomas A. Drake.*" I think it is important to point out that my process in addressing your complaint examined (and distinguished between) the classification of the document in its first instance and any continuation of its classification "in the matter of *United States v. Thomas A. Drake*." I find no violation in either case. In fact, as materials you provided with your complaint make clear, NSA discontinued the classification of the document in question and represented the same to the court "in the matter of *United States v. Thomas A. Drake*."

In examining the "What a Wonderful Success" document, I find that the NSA did not violate the Order's requirements for appropriately applying classification at document creation, nor did the agency violate the Order's expectation that information shall be declassified when it no longer meets the standards for classification. While my examination of the matter has led to my conclusion that the content and processing of the document fall within the standards and authority for classification under the Order and NSA regulations, that does not make them immune to opinions about how substantial the document's content may or may not be. I find, simply, that those opinions do not rise to the level of willful acts in violation of the Order. That said, such commentary on the culture of classification fits well in discussions of policy reform. In such fora, including the work of the Public Interest Declassification Board, your experience and observations would continue to be welcome.

Separate and apart from the specifics of the Drake matter, there are important aspects of the classification system worth noting in this larger discussion of the scope of classification guidance. As you are aware, section 1.1 of the Order grants both responsibility and latitude to Executive branch officials with original classification authority. These officials are the chief subject matter experts in government concerning information that could be damaging to national security if compromised or released in an unauthorized manner.

In light of this, section 2.2 of the Order directs officials with original classification authority to prepare classification guides to facilitate the proper and uniform classification of information. A well-constructed classification guide can foster consistency and accuracy throughout a very large agency, can impart direction concerning the duration of classification, and ensure that information is properly identified and afforded necessary

Roark v. U.S., Attachment 2

protections. Throughout the Executive branch, officials strive to impart proper classification guidance that is accurate, consistent, and easy to adopt in workforces that operates under tight time constraints. It seems quite clear, however, that the system would benefit from greater attention of senior officials in ensuring that their guidance applies classification only to information that clearly meets all classification standards in section 1.1 of the Order. For emphasis, I draw specific attention to language in Section 1.1 (a)(4) "... that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security..." and, 1.1 (b) "If there is significant doubt about the need to classify information, is shall not be classified."

I have a few observations about these matters in the context in which you raised them, namely, the matter of the *United States v Thomas A. Drake*. I have no basis to comment about the disposition of the case in the courts; that is not my purview. The conduct of the case did, however, bring to light actions and behaviors I will comment on briefly, for emphasis. The Order does not grant any individual the authority to safeguard classified information in a manner that is contrary to what the Order, its implementing directive, or an agency's security regulations require. The Order does not grant authorized holders of classified information the authority to make their own decisions concerning the classification status of that information. Furthermore, individuals are provided the means to challenge classification either formally or informally. Section 1.8 of the Order provides all authorized holders of classified information with the authority to issue challenges to classification actions. It explicitly states that individuals are "encouraged and expected" to challenge the classification status of the information through appropriate channels, and every agency is required to implement procedures whereby any authorized holder may issue a challenge without fear of retribution. I know, through the work of this Office, that the National Security Agency is well practiced in the Order's requirements concerning classification challenges. It is my understanding that Mr. Drake made no attempts to challenge the classification status of the information in question.

I note that neither version of the Order in force during the Drake case's time frame [Executive Order 13526 (29 December 2009) and its predecessor Executive Order 12958 (17 April 1995)] provides much in the way of guidance or direction, on its own, to influence the use of classified information in building prosecutions such as this. In general, the Department of Justice defers to the judgment of the "victim" agency as to what constitutes classified information. In building a case, victim agencies, for their part, tend to provide evidence that they deem sufficient to obtain a conviction with the hopes of protecting their most sensitive information and activities from release during court proceedings. The Directive (32 CFR 2001.48) requires only that agency heads "use established procedures to ensure coordination with" the Department of Justice and other counsel. All of this assumes that other influences will be at work to pursue only worthwhile prosecutions, but one interpretation of the Drake case outcome might suggest that this "coordination" was not sufficient. I would welcome your thoughts on whether there is role for policy to provide clearer, more effective guidance in the manner in which such cases are built.

I thank you for your diligent, care-filled observations and comments concerning classification matters. You continue to serve the public well by remaining engaged in the dialogue around the use of secrecy by the government. I can assure you that we take these viewpoints to heart.

Sincerely,

<Signed>

JOHN P. FITZPATRICK
Director, Information Security Oversight Office

From: Bill Leonard
Date: December 31, 2012, 4:10:23 PM EST
To: John Fitzpatrick
Subject: Re: Complaint

John:

Thanks very much for your reply. While I appreciate the time, effort and consideration you put into this matter, I am nonetheless disappointed in the substance of your reply. Some of my final thoughts on this matter include:

1. It took almost one and a half years to respond to a rather straightforward yet serious request. I recognize the need for coordination; nonetheless, irrespective of the nature of the reply, responsiveness is essential for a system to be able to be self-correcting.

2. As we discussed when we met in August 2011, I have never taken real issue with the classification of the "What a Success" document in the first instance, which although improper was, by all appearances, a reflexive rather than willful act. Nor did I take issue with its eventual "declassification," which I regarded as NSA simply coming to the proper conclusion, albeit belatedly. What I did and continue to take issue with is that in between those events, senior officials of both the NSA and DoJ made a number of deliberate decisions to use the supposed classified nature of that document as the basis for a criminal investigation of Thomas Drake as well as the basis for a subsequent felony indictment and criminal prosecution. Even after NSA recognized that the document did not meet the standards for continued classification and made the unprecedented decision to declassify an evidentiary document while an Espionage Act criminal prosecution was still pending, senior officials of both the NSA and DoJ still willfully persisted and made yet another deliberate decision to stand by the document's original classification status. I cannot imagine a clearer indication of willfulness on the part of senior government officials to "continue the classification of information in violation" of the governing order through numerous deliberate and collaborative decisions made over the course of years. Based upon my extensive experience, I find the provenance of this document's classification status to be unparalleled in the history of criminal prosecutions under the Espionage Act.

3. You ascribe the merits of my complaint as constituting a mere honest difference in opinion. However, this complaint is more than a question of the document failing to pass what I call the "guffaw test" (i.e. common sense). Rather, as I pointed out in my original complaint and yet you did not address, at the heart of this issue are matters of fact. In justifying the deliberate decision to represent during the Drake prosecution that the "What a Success" email was a legitimately classified document, NSA and DoJ officials did not cite some amorphous classification standard or classification guide - rather they made factual representations which simply were not true and, in one instance, inherently contradictory (i.e. "information contained therein **reveals ... a specific level** (emphasis added) of effort ..."

Roark v. U.S., Attachment 2

and that the same information **"implied a level** (emphasis added) of effort ..."). Keep in mind that these determinations were not made on the fly by NSA and DoJ but were in fact deliberate representations made over a period of time and subsequently further qualified but never disavowed. They were intended to demonstrate that the document met the standards of classification that require the original classification authority to identify or describe the damage to national security that could reasonably be expected to result from the unauthorized disclosure. A familiarity with classification standards is not required to determine that these official representations were on their face factually incorrect when compared with a plain text reading of the "What a Success" email. All too often, representatives of the Executive branch believe all they need to do is simply assert classification rather than adhere to the president's own standards, as apparently was the situation in the Drake case. That attitude must change and I will continue to do all I can to help make it foster change.

4. You comment on the fact that the Order does not grant any individual the authority to handle classified information in a manner contrary to the Order and other pertinent regulations. While reference to alleged actions taken or not taken by Mr. Drake are gratuitous and have no bearing on the merits of my complaint, I nonetheless agree with your sentiment. However, allow me to add my own observations, not only as one of your predecessors but also as the only individual who has played an integral role for both defense teams in the only two Espionage Act prosecutions (Drake and AIPAC) not to result in either a conviction or a plea of guilty. In both instances (in which I provided my services pro bono) my decision to get involved was not to defend the actions of the accused but rather to defend the integrity of the classification system, a highly critical national security tool. I have long held that when government agencies fail to adhere to their responsibilities under the governing order and implementing directive, they in turn compromise their ability to hold cleared individuals accountable for their actions. Accountability is crucial to any system of controls and the fact that your determination in this case preserves an unbroken record in which no government official has ever been held accountable for abusing the classification system does not bode well for the prospect of real reform of the system. This phenomenon, the readily apparent inclusion in the Order of a feckless provision which infers that accountability cuts both ways has once again been proven to be a major source of why most informed observers both inside and outside the government recognize that the classification system remains dysfunctional due to rampant and unchecked over-classification. It is disappointing to note that a genuine opportunity to instill an authentic balance to the system has been forfeited in this instance.

As to your request for my recommendations as to the potential for clearer guidance when the classification status of information is integral to a criminal prosecution, I would recommend requiring coordination with an independent body such as the Interagency Security Classification Appeals Panel. In the two cases I referenced above, the fact that the government did not obtain a criminal conviction under the Espionage Act actually bode well for the integrity of the classification system -- otherwise, the perceived wisdom in the reflexive over-classification of information would have been codified in case law.

Finally, I stand ready to share my experiences and observations with the Public Interest

Declassification Board and other fora as seen fit.

Thanks again for the reply, John. While I admire the job you do and the challenges you face, I obviously disagree with the content of your reply. Nonetheless, I am appreciative of the courtesy.

Best wishes for the New Year.

jwl

GENERAL AFFIDAVIT

State of Maryland
County of Carroll

BEFORE ME, the undersigned Notary, Cheryl A. Smith, on this 12th day of January 2015, personally appeared William E. Binney, known to me to be a credible person and of lawful age, who being by me first duly sworn, on his oath, deposes and says:

In the matter of a 12 – 14 page document referred to as the THIN THREAD paper, the U.S. Government, through its agent, the U.S. Department of Justice, and in the person of Assistant U.S. Attorney Thomas H. Barnard, District of Maryland, in a meeting held in July or August of 2012 at the District Court of Maryland, did state it had no interest in other copies of said document in the public domain, which is contrary to U.S. Government policy for the safeguarding and security of media and information the government deems classified.

In a related matter, William E. Binney sent a copy of said document to Mr. James Picard of Robbins-Gioia, LLC in 2007. This document was not treated as sensitive information, despite the fact John K. Wiebe notified James Picard of the U.S. Government's claim the paper was sensitive. Mr. Picard notified his security staff at his company, but neither the document nor the hard drive on which he placed it was removed, according to a phone conversation John K. Wiebe had with Mr. Picard some weeks later. Such behavior is contrary to U.S. Government policy for the safeguarding and security of media and information the Government deems sensitive. I can only conclude that the Thin Thread paper was, in fact, not sensitive at all. This would be consistent with the evidence presented in Maryland district court in a 41G law suite against the government for return of property by Kirk Wiebe, William Binney, Edward Loomis and Thomas Drake.

I hereby state that the information stated herein is true, to the best of my knowledge. I also state that the information put forth here is both accurate and complete.

[signature of William E. Binney]

William E. Binney
7800 Elberta Drive

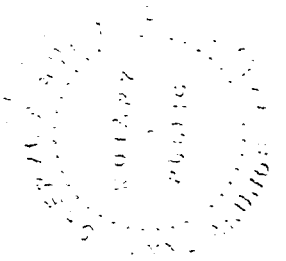
Severn, Md 21144

Subscribed and sworn to before me, this 12 *[day of month]* day of January, 2015.

Subscribed and sworn to before me, in my presence
this 12 day of Jan 2015 a Notary Public
in and for the STATE of Maryland
Cheryl A. Smith
My commission expires Nov 13 2018

Roark v. U.S.
Attachment 3

[Notary Seal:]



Cheryl A. Smith

[signature of Notary]

Cheryl A. Smith

[typed name of Notary]

NOTARY PUBLIC

My commission expires: Nov 13, 2018.

GENERAL AFFIDAVIT

State of Maryland
County of Carroll

BEFORE ME, the undersigned Notary, Anna Miranda, on this 12th day of January 2015, personally appeared John K. Wiebe, known to me to be a credible person and of lawful age, who being by me first duly sworn, on his oath, deposes and says:

In the matter of a 12 – 14 page document referred to as "the THIN THREAD paper", the U.S. Government, through its agent, the U.S. Department of Justice, and in the person of Assistant U.S. Attorney Thomas H. Barnard, District of Maryland, in a meeting held in July or August of 2012 at the District Court of Maryland, did state it had no intent to retrieve all available copies of said document, which is contrary to U.S. Government policy for the safeguarding and security of media and information the government deems classified.

In a related matter, a copy of said document sent to Mr. James Picard of Robbins-Gioia, LLC by William E. Binney in 2007 was not treated as classified information, despite the fact I notified Mr. Picard of the U.S. Government's claim the paper was classified. Mr. Picard notified his security staff at his company, but neither the document nor the hard drive on which he placed it was removed from his computer, according to a phone conversation I had with Mr. Picard some weeks later. Such behavior is contrary to U.S. Government policy for the safeguarding and security of media and information the Government deems classified.

In addition, I certify that in the matter of the 26 July 2007 seizure by the FBI and subsequent return of personal information that had been stored on computer hard drives belonging to me, the Government did in fact return to me the very same document referred to as "the THIN THREAD paper" on two separate occasions. The first occasion occurred in 2009 when the FBI returned to me an external hard drive I used as a backup storage disc. The second occurred in 2013 when the FBI returned personal information that had been stored on the hard drives retained by the FBI. Return of the information was carried out subsequent to the ruling of Judge Richard D. Bennett in the case *John Wiebe, et al. v. National Security Agency* heard in the Maryland District Court, Baltimore, MD. Return of information the Government has claimed is classified or "sensitive" is contrary to U.S. Government policy for the safeguarding and security of classified and otherwise "sensitive" information. Perhaps more importantly, the return of the paper, including two copies at different times, indicates that the paper was neither classified nor "unclassified-but-sensitive" information.

I hereby state that the information stated herein is true, to the best of my knowledge. I also state that the information put forth here is both accurate and complete.

Roark v. U.S.
Attachment 3

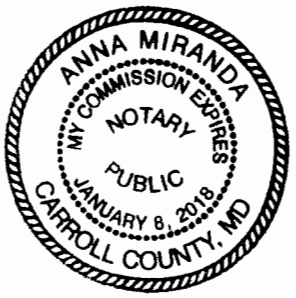
John K. Wiebe

1390 Alison Court

Westminster, MD 21158-2741

Subscribed and sworn to before me, this 12th day of January, 2015.

[Notary Seal:]



[signature of Notary]

Anna Miranda

[typed name of Notary]

NOTARY PUBLIC

My commission expires: January 8, 2018.

Affidavit for Diane Roark
from
Thomas Drake

15 Jan 2015

RE: Return of Seized Property by the FBI

State of Maryland, County of Howard

Before the undersigned, an officer duly commissioned by the laws of Maryland, on this 15 day of January, 2015, personally appeared Thomas A. Drake who having first duly sworn and says:

After the conclusion of my criminal case in July 2011, a civil lawsuit was filed by William Binney, J. Kirk Wiebe, Edward Loomis, and myself against the NSA, DoJ and FBI for the return of property seized by the FBI during raids of our residences within the period of July-November 2007.

Upon examination of the returned materials seized by the FBI from my residence in November 2007, I was unable to find any of the documents or related material from the charging or supporting documents in my criminal case, and was unable to find any correspondence related to the THINTHREAD (TT) paper from the period of April-July 2002 and Jan-April 2006 or the Diane Roark op-ed draft from July-October 2006, as all were apparently retained by the government as "protected information" from disclosure.

Prior to my indictment, the government focused on the TT paper for a long time as one of the key documents in their criminal investigation of me, but this same paper was not in the indictment, and instead they fabricated evidence by retroactively classifying 5 unclassified papers that formed the basis of the Espionage Act charges against me.

In summary I had copies of the Diane Roark OpEd (as well as the TT paper) but they were never raised as a classification issue (nor were the documents ever designated as charging or supporting documents, during my criminal case), after I was indicted by the Department of Justice in April 2010. And none of this material was ever provided as part of the criminal proceedings against me during the period of April 2010-July 2011.

Thomas A. Drake

Subscribed and sworn to before me this 15 day of January, 2015.

Notary Public

My Commission Expires on: Nov. 20, 2018

Roark v. U.S.
Attachment 3

Roark v. U.S. Attachment 4

Plan Aims to Ease Agencies' Sharing to Curb Attacks

By Cam Simpson And Siobhan Gorman

12-15-09

WASHINGTON—The Obama administration will announce Tuesday that it plans to make it easier for local, state and federal authorities to share clues that could thwart potential terrorist attacks.

At issue are the reams of reports, guidelines and advisories produced across the government every day that aren't sensitive enough to get classifications such as "top secret," but are still too sensitive to make immediately available to the public.

Right now, government agencies use a tangle of more than 100 categories for this sort of sensitive information. By one count, there are 117. Many of the categories have their own rules for how the information can be shared both inside and among agencies.

That red tape can contribute to keeping information from officials who could help connect dots and deter a terrorist attack, officials said.

President Barack Obama has ordered his staff to craft an executive order to consolidate those categories down to one, "Controlled Unclassified Information," according to a White House official involved in the effort.

The executive order will also create a standardized set of rules for handling and sharing such data within all agencies, the official said.

The Obama administration also will announce that it is expanding a program that collects and analyzes potential terrorism tips from local police officers, so that, by 2014, all states will have the capability to analyze that data and share it with other states and the federal government, a senior homeland security official said.

Associated Press

Attorney General Eric Holder testifies to Congress in November.

The effort will take two to four years because it involves training analysts and setting up technology in 50 states, officials said.

Mr. Obama in May asked Homeland Security Secretary Janet Napolitano and Attorney General Eric Holder to lead a task force to study barriers to sharing sensitive information that still exist more than eight years after the Sept. 11, 2001, terrorist attacks. The failure of agencies to share information about the Sept. 11 hijackers and the conspiracy was later seen as a serious problem across the government.

The effort could become more urgent in the face of a spate of cases this year involving home-grown terrorist threats. The report, which has 40 recommendations, is scheduled to be released Tuesday. Key aspects are expected to serve as a basis for Mr. Obama's executive order.

One example of sensitive information: a Transportation Security Administration manual leaked last week that tells airport screeners across the nation what to look for when travelers pass through their security checkpoints.

Although not classified, the report was considered too sensitive to release publicly because it could give clues to anyone who wants to smuggle something dangerous onto an airliner.

The executive order will also aim to make such information more readily available to the public when it is no longer sensitive, the White House official said. Officials said they would announce Tuesday their intent to protect information "only where there is a compelling requirement to do so."

The most critical aspect of the new policy will be how the administration defines its new category, Controlled Unclassified Information, said Steven Aftergood, a government-secrecy specialist at the Federation of American Scientists.

Early drafts of the definition, he said, included loopholes that could allow agencies to restrict access to any information they chose just by rewriting agency policy.

Another key issue will be implementation of the policy. One reason so many government documents have been labeled as sensitive is that employees felt their work was too important to share widely, and it isn't clear how the Obama administration's policy will change that, Mr. Aftergood said.

"I'm not sure that the problem that drove the creation of the 117 categories [of sensitive information] has been solved," he said, "but I admire the attempt."

Wall St. Journal

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release May 27, 2009

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Classified Information and Controlled Unclassified Information

As outlined in my January 21, 2009, memoranda to the heads of executive departments and agencies on Transparency and Open Government and on the Freedom of Information Act, my Administration is committed to operating with an unprecedented level of openness. While the Government must be able to prevent the public disclosure of information where such disclosure would compromise the privacy of American citizens, national security, or other legitimate interests, a democratic government accountable to the people must be as transparent as possible and must not withhold information for self-serving reasons or simply to avoid embarrassment.

To these ends, I hereby direct the following:

Section 1. Review of Executive Order 12958. (a) Within 90 days of the date of this memorandum, and after consulting with the relevant executive departments and agencies (agencies), the Assistant to the President for National Security Affairs shall review Executive Order 12958, as amended (Classified National Security Information), and submit to me recommendations and proposed revisions to the order.

(b) The recommendations and proposed revisions shall address:

(i) Establishment of a National Declassification Center to bring appropriate agency officials together to perform collaborative declassification review under the administration of the Archivist of the United States;

(ii) Effective measures to address the problem of over classification, including the possible restoration of the presumption against classification, which would preclude classification of information where there is significant doubt about the need for such classification, and the implementation of increased accountability for classification decisions;

(iii) Changes needed to facilitate greater sharing of classified information among appropriate parties;

(iv) Appropriate prohibition of reclassification of material that has been declassified and released to the public under proper authority;

(v) Appropriate classification, safeguarding, accessibility, and declassification of information in the electronic environment, as recommended by the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction and others; and

(vi) Any other measures appropriate to provide for greater openness and transparency in the Government's security classification and declassification program while also affording necessary protection to the Government's legitimate interests.

Sec. 2. Review of Procedures for Controlled Unclassified Information. (a) Background. There has been a recognized need in recent years to enhance national security by establishing an information sharing environment that facilitates the sharing of terrorism-related information among government personnel addressing common problems across agencies and levels of government. The global nature of the threats facing the United States requires that our Nation's entire network of defenders be able rapidly to share sensitive but unclassified information so that those who must act have the information they need.

To this end, efforts have been made to standardize procedures for designating, marking, and handling information that had been known collectively as "Sensitive But Unclassified" (SBU) information. Sensitive But Unclassified refers collectively to the various designations used within the Federal Government for documents

LATEST BLOG POSTS

January 12, 2015 6:01 PM EST

The President Announces New Actions to Protect Americans' Privacy and Identity

President Obama stops by the Federal Trade Commission offices to talk about how we can better protect consumers from identity theft and safeguard everyone's privacy, including our children.

January 12, 2015 5:45 PM EST

Email from Dan Pfeiffer: "Your Memo for the President"

White House Senior Advisor Dan Pfeiffer announces an opportunity for the public to voice their concerns for the 2015's "Citizens Memo." The memo will be constructed from comments sent through the online form listed and will outline goals for the end of the Obama administration.

January 12, 2015 2:08 PM EST

2015 SelectUSA Investment Summit Is Now Open for Business

At the 2015 SelectUSA Investment Summit, economic development organizations (EDOs) from across the United States will once again gather to showcase investment opportunities to companies from around the world.

VIEW ALL RELATED BLOG POSTS

Facebook YouTube

Twitter Vimeo

Flickr iTunes

Google+ LinkedIn

Roark v. U.S.
Attachment 4

and information that are sufficiently sensitive to warrant some level of protection, but that do not meet the standards for national security classification. Because each agency has implemented its own protections for categorizing and handling SBU, there are more than 107 unique markings and over 130 different labeling or handling processes and procedures for SBU information.

A Presidential Memorandum of December 16, 2005, created a process for establishing a single, standardized, comprehensive designation within the executive branch for most SBU information. A related Presidential Memorandum of May 9, 2008 (hereafter the "May 2008 Presidential Memorandum"), adopted the phrase "Controlled Unclassified Information" (CUI) to refer to such information. That memorandum adopted, instituted, and defined CUI as the single designation for information within the scope of the CUI definition, including terrorism-related information previously designated SBU. The memorandum also established a CUI Framework for designating, marking, safeguarding, and disseminating CUI terrorism-related information; designated the National Archives and Records Administration as the Executive Agent responsible for overseeing and managing implementation of the CUI Framework, and created a CUI Council to perform an advisory and coordinating role.

The May 2008 Presidential Memorandum had the salutary effect of establishing a framework for standardizing agency-specific approaches to designating terrorism-related information that is sensitive but not classified. As anticipated, the process of implementing the new CUI Framework is still ongoing and is not expected to be completed until 2013. Moreover, the scope of the May 2008 Presidential Memorandum is limited to terrorism-related information within the information sharing environment. In the absence of a single, comprehensive framework that is fully implemented, the persistence of multiple categories of SBU, together with institutional and perceived technological obstacles to moving toward an information sharing culture, continue to impede collaboration and the otherwise authorized sharing of SBU information among agencies, as well as between the Federal Government and its partners in State, local, and tribal governments and the private sector.

Agencies and other relevant actors should continue their efforts toward implementing the CUI framework. At the same time, new measures should be considered to further and expedite agencies' implementation of appropriate frameworks for standardized treatment of SBU information and information sharing.

(b) Interagency Task Force on CUI.

(i) The Attorney General and the Secretary of Homeland Security, in consultation with the Secretary of State, the Archivist of the United States, the Director of the Office of Management and Budget, the Director of National Intelligence, the Program Manager, Information Sharing Environment (established in section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, as amended (6 U.S.C. 485)), and the CUI Council (established in the May 2008 Presidential Memorandum), shall lead an Interagency Task Force on CUI (Task Force). The Task Force shall be composed of senior representatives from a broad range of agencies from both inside and outside the information sharing environment.
(ii) The objective of the Task Force shall be to review current procedures for categorizing and sharing SBU information in order to determine whether such procedures strike the proper balance among the relevant imperatives. These imperatives include protecting legitimate security, law enforcement, and privacy interests as well as civil liberties, providing clear rules to those who handle SBU information, and ensuring that the handling and dissemination of information is not restricted unless there is a compelling need. The Task Force shall also consider measures to track agencies' progress with implementing the CUI Framework, other measures to enhance implementation of an effective information sharing environment across agencies and levels of government, and whether the scope of the CUI Framework should remain limited to terrorism-related information within the information sharing environment or be expanded to apply to all SBU information.

(iii) Within 90 days of the date of this memorandum, the Task Force shall submit to me recommendations regarding how the executive branch should proceed with respect to the CUI Framework and the information sharing environment. The recommendations shall recognize and reflect a balancing of the following principles:

(A) A presumption in favor of openness in accordance with my memoranda of January 21, 2009, on Transparency and Open Government and on the Freedom of Information Act;
(B) The value of standardizing the procedures for designating, marking, and handling all SBU information; and

(C) The need to prevent the public disclosure of information where disclosure would compromise privacy or other legitimate interests.

Sec. 3. General Provisions. (a) The heads of agencies shall assist and provide information to the Task Force, consistent with applicable law, as may be necessary to carry out the functions of their activities under this memorandum. Each agency shall bear its own expense for participating in the Task Force.

(b) Nothing in this memorandum shall be construed to impair or otherwise affect:

(i) Authority granted by law or Executive Order to an agency, or the head thereof;
(ii) Functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(c) This memorandum shall be implemented consistent with applicable law and subject to the availability of appropriations.

(d) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

Sec. 4. Publication. The Attorney General is hereby authorized and directed to publish this memorandum in the Federal Register.

The White House

Office of the Press Secretary

For Immediate Release November 04, 2010

Executive Order 13556 -- Controlled Unclassified Information

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose. This order establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

At present, executive departments and agencies (agencies) employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. The fact that these agency-specific policies are often hidden from public view has only aggravated these issues.

To address these problems, this order establishes a program for managing this information, hereinafter described as Controlled Unclassified Information, that emphasizes the openness and uniformity of Government-wide practice.

Sec. 2. Controlled Unclassified Information (CUI).

(a) The CUI categories and subcategories shall serve as exclusive designations for identifying unclassified information throughout the executive branch that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.

(b) The mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to any law requiring the disclosure of information or permitting disclosure as a matter of discretion, including disclosures to the legislative or judicial branches.

(c) The National Archives and Records Administration shall serve as the Executive Agent to implement this order and oversee agency actions to ensure compliance with this order.

Sec. 3. Review of Current Designations.

(a) Each agency head shall, within 180 days of the date of this order:

(1) review all categories, subcategories, and markings used by the agency to designate unclassified information for safeguarding or dissemination controls; and

(2) submit to the Executive Agent a catalogue of proposed categories and subcategories of CUI, and proposed associated markings for information designated as CUI under section 2(a) of this order. This submission shall provide definitions for each proposed category and subcategory and identify the basis in law, regulation, or Government-wide policy for safeguarding or dissemination controls.

(b) If there is significant doubt about whether information should be designated as CUI, it shall not be so designated.

Sec. 4. Development of CUI Categories and Policies.

LATEST BLOG POSTS

January 12, 2015 6:01 PM EST

The President Announces New Actions to Protect Americans' Privacy and Identity

President Obama stops by the Federal Trade Commission offices to talk about how we can better protect consumers from identity theft and safeguard everyone's privacy, including our children.

January 12, 2015 5:45 PM EST

Email from Dan Pfeiffer: "Your Memo for the President"

White House Senior Advisor Dan Pfeiffer announces an opportunity for the public to voice their concerns for the 2015's "Citizens Memo." The memo will be constructed from comments sent through the online form listed and will outline goals for the end of the Obama administration.

January 12, 2015 2:08 PM EST

2015 SelectUSA Investment Summit Is Now Open for Business

At the 2015 SelectUSA Investment Summit, economic development organizations (EDOs) from across the United States will once again gather to showcase investment opportunities to companies from around the world.

VIEW ALL RELATED BLOG POSTS

Facebook YouTube

Twitter Vimeo

Flickr iTunes

Google+ LinkedIn

Roark v. U.S.
Attachment 4

(a) On the basis of the submissions under section 3 of this order or future proposals, and in consultation with affected agencies, the Executive Agent shall, in a timely manner, approve categories and subcategories of CUI and associated markings to be applied uniformly throughout the executive branch and to become effective upon publication in the registry established under subsection (d) of this section. No unclassified information meeting the requirements of section 2(a) of this order shall be disapproved for inclusion as CUI, but the Executive Agent may resolve conflicts among categories and subcategories of CUI to achieve uniformity and may determine the markings to be used.

(b) The Executive Agent, in consultation with affected agencies, shall develop and issue such directives as are necessary to implement this order. Such directives shall be made available to the public and shall provide policies and procedures concerning marking, safeguarding, dissemination, and decontrol of CUI that, to the extent practicable and permitted by law, regulation, and Government-wide policies, shall remain consistent across categories and subcategories of CUI and throughout the executive branch. In developing such directives, appropriate consideration should be given to the report of the interagency Task Force on Controlled Unclassified Information published in August 2009. The Executive Agent shall issue initial directives for the implementation of this order within 180 days of the date of this order.

(c) The Executive Agent shall convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

(d) Within 1 year of the date of this order, the Executive Agent shall establish and maintain a public CUI registry reflecting authorized CUI categories and subcategories, associated markings, and applicable safeguarding, dissemination, and decontrol procedures.

(e) If the Executive Agent and an agency cannot reach agreement on an issue related to the implementation of this order, that issue may be appealed to the President through the Director of the Office of Management and Budget.

(f) In performing its functions under this order, the Executive Agent, in accordance with applicable law, shall consult with representatives of the public and State, local, tribal, and private sector partners on matters related to approving categories and subcategories of CUI and developing implementing directives issued by the Executive Agent pursuant to this order.

Sec. 5. Implementation.

(a) Within 180 days of the issuance of initial policies and procedures by the Executive Agent in accordance with section 4(b) of this order, each agency that originates or handles CUI shall provide the Executive Agent with a proposed plan for compliance with the requirements of this order, including the establishment of interim target dates.

(b) After a review of agency plans, and in consultation with affected agencies and the Office of Management and Budget, the Executive Agent shall establish deadlines for phased implementation by agencies.

(c) In each of the first 5 years following the date of this order and biennially thereafter, the Executive Agent shall publish a report on the status of agency implementation of this order.

Sec. 6. General Provisions.

(a) This order shall be implemented in a manner consistent with:

(1) applicable law, including protections of confidentiality and privacy rights;

(2) the statutory authority of the heads of agencies, including authorities related to the protection of information provided by the private sector to the Federal Government; and

(3) applicable Government-wide standards and guidelines issued by the National Institute of Standards and Technology, and applicable policies established by the Office of Management and Budget.

(b) The Director of National Intelligence (Director), with respect to the Intelligence Community and after consultation with the heads of affected agencies, may issue such policy directives and guidelines as the Director deems necessary to implement this order with respect to intelligence and intelligence-related information. Procedures or other guidance issued by Intelligence Community element heads shall be in accordance with such policy directives or guidelines issued by the Director. Any such policy directives or guidelines issued by the Director shall be in accordance with this order and directives issued by the Executive Agent.

(c) This order shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, and legislative proposals.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable

(a) On the basis of the submissions under section 3 of this order or future proposals, and in consultation with affected agencies, the Executive Agent shall, in a timely manner, approve categories and subcategories of CUI and associated markings to be applied uniformly throughout the executive branch and to become effective upon publication in the registry established under subsection (d) of this section. No unclassified information meeting the requirements of section 2(a) of this order shall be disapproved for inclusion as CUI, but the Executive Agent may resolve conflicts among categories and subcategories of CUI to achieve uniformity and may determine the markings to be used.

(b) The Executive Agent, in consultation with affected agencies, shall develop and issue such directives as are necessary to implement this order. Such directives shall be made available to the public and shall provide policies and procedures concerning marking, safeguarding, dissemination, and decontrol of CUI that, to the extent practicable and permitted by law, regulation, and Government-wide policies, shall remain consistent across categories and subcategories of CUI and throughout the executive branch. In developing such directives, appropriate consideration should be given to the report of the interagency Task Force on Controlled Unclassified Information published in August 2009. The Executive Agent shall issue initial directives for the implementation of this order within 180 days of the date of this order.

(c) The Executive Agent shall convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

(d) Within 1 year of the date of this order, the Executive Agent shall establish and maintain a public CUI registry reflecting authorized CUI categories and subcategories, associated markings, and applicable safeguarding, dissemination, and decontrol procedures.

(e) If the Executive Agent and an agency cannot reach agreement on an issue related to the implementation of this order, that issue may be appealed to the President through the Director of the Office of Management and Budget.

(f) In performing its functions under this order, the Executive Agent, in accordance with applicable law, shall consult with representatives of the public and State, local, tribal, and private sector partners on matters related to approving categories and subcategories of CUI and developing implementing directives issued by the Executive Agent pursuant to this order.

Sec. 5. Implementation.

(a) Within 180 days of the issuance of initial policies and procedures by the Executive Agent in accordance with section 4(b) of this order, each agency that originates or handles CUI shall provide the Executive Agent with a proposed plan for compliance with the requirements of this order, including the establishment of interim target dates.

(b) After a review of agency plans, and in consultation with affected agencies and the Office of Management and Budget, the Executive Agent shall establish deadlines for phased implementation by agencies.

(c) In each of the first 5 years following the date of this order and biennially thereafter, the Executive Agent shall publish a report on the status of agency implementation of this order.

Sec. 6. General Provisions.

(a) This order shall be implemented in a manner consistent with:

(1) applicable law, including protections of confidentiality and privacy rights;

(2) the statutory authority of the heads of agencies, including authorities related to the protection of information provided by the private sector to the Federal Government; and

(3) applicable Government-wide standards and guidelines issued by the National Institute of Standards and Technology, and applicable policies established by the Office of Management and Budget.

(b) The Director of National Intelligence (Director), with respect to the Intelligence Community and after consultation with the heads of affected agencies, may issue such policy directives and guidelines as the Director deems necessary to implement this order with respect to intelligence and intelligence-related information. Procedures or other guidance issued by Intelligence Community element heads shall be in accordance with such policy directives or guidelines issued by the Director. Any such policy directives or guidelines issued by the Director shall be in accordance with this order and directives issued by the Executive Agent.

(c) This order shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, and legislative proposals.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable

at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(e) This order shall be implemented subject to the availability of appropriations.

(f) The Attorney General, upon request by the head of an agency or the Executive Agent, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(g) The Presidential Memorandum of May 7, 2008, entitled "Designation and Sharing of Controlled Unclassified Information (CUI)" is hereby rescinded.

BARACK OBAMA

THE WHITE HOUSE,
November 4, 2010.

at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(e) This order shall be implemented subject to the availability of appropriations.

(f) The Attorney General, upon request by the head of an agency or the Executive Agent, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(g) The Presidential Memorandum of May 7, 2008, entitled "Designation and Sharing of Controlled Unclassified Information (CUI)" is hereby rescinded.

BARACK OBAMA

THE WHITE HOUSE,
November 4, 2010.